sending data comprising the encrypted application key to the second unit;

on each downloading, computing an operation key in the second unit based on information specific to the second unit, the transport key and the diversification algorithm, the same transport key residing in the non-volatile memory of each second security unit of said set, said operation key not being stored within the memory of said second unit; and

A1 cncld.

decrypting the encrypted application key in the second unit based on information comprising said operation key and a decryption algorithm which is the inverse of the encryption algorithm.

21. (New) A method according to claim 3, further comprising:

sending the random information, information pertaining to an application key and information specific to the second unit to the first unit by means of a first single command.

22. (New) A method according to claim 4, further comprising:

sending the random information, information pertaining to an application key and information specific to the second unit to the first unit by means of a first single command.

23. (New) A method according to claim 2, further comprising:

sending the encrypted application key and the information pertaining to an application key to the second unit by means of a single second command.--

Please amend the claims as follows:

2. (Once Amended) A method according to claim 20, further comprising:

sending information specific to the second unit to the first unit before computing the application key in the first unit.

A2 Cn't

3. (Once Amended) A method according to claim 20, further comprising:

sending a random number provided by the second unit to the first unit, before encrypting the application key in the first unit.

4. (Once Amended) A method according to claim 20, further comprising:

sending information pertaining to an application key to the first unit, before encrypting the application key within said first unit.

5. (Once Amended) A method according to claim 4, further comprising:

choosing the application key to be encrypted based on said information.

6. (Once Amended) A method according to claim 20, wherein said encryption of an application key intended for a second unit is unique.

7. (Once Amended) A method according to claim 20, further comprising:

verifying integrity of the data includes the encrypted application key.

8. (Once Amended) A method according to claim 20, further comprising:

sending information pertaining to an application key to the second unit, before decrypting the encrypted application key within said second unit of said set.

9. (Once Amended) A method according to claim 20, further comprising:

storing within the second unit, after decrypting the encrypted application key, said key within said second unit.

10. (Once Amended) A method according to claim 9, wherein storing of the application key within the second unit is done based on information pertaining to an application key.

11. (Once Amended) A method according to claim 20, further comprising:

verifying that the application key is authentic.

12. (Once Amended) A method according to claim 20, wherein the first security unit comprises a smart card.

13. (Once Amended) A method according to claim 20, wherein the memory comprises a rewritable memory.

14. (Once Amended) A method according to claim 20, wherein a second unit comprises several application keys.

15. (Once Amended) A method according to claim 20, wherein the first unit comprises several application keys.

16. (Once Amended) A method according to claim 20, further comprising:

after encrypting the application key, erasing the operation key temporarily saved within the second volatile memory of the first unit.

17. (Once Amended) A method according to claim 20, further comprising: